International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 6, Issue 2, Apr 2016, 41-50

PUPIL DILATIONS DETECT IRIS LIVENESS DETECTION

PASUPULETI LP BHARATI[1] & KEZIA RANI BADITHI[2]

[1]*Reaserch Scholar, College of Engineering, Adikavi Nannaya University, Rajahmundry, Andhra Pradesh, India*

[2]*Assistant Professor, College of Engineering, Adikavi Nannaya University, Rajahmundry, Andhra Pradesh, India*

ABSTRACT

In today's computerized society, impostors are gaining access when compared to real authorized users. Spoofing biometric systems to gain unauthorized access is the main concept of impostor. Spoofing is the process of defeating a biometric system through the introduction of fake biometric samples. It is a method of fooling biometric system, where fake objects are presented to the scanner which imitates unique properties as authenticators, thereby fooling it from distinguishing artifact from real target. People leave finger prints everywhere in day to day lives. Faces and irises are visible to everyone and voices can be recorded. So, the chance of someone lifting and copying them to replicate for the purpose of spoofing may be possible. Hence it is considered as a challenging threat to Biometric systems. Liveness Detection is considered as the most anti spoofing method for protecting genuine authentications from impostors. It is done mainly under three categories: Intrinsic properties of living body, involuntary signals of living body, and Bodily responses to external stimuli. Eye blinks and pupil dynamics are considered for morphological traits of Iris, and characteristics like red eye effect, Purkinje images etc are mentioned for dynamics liveness detection. In this paper, target biometric traits for spoofing are mentioned and various methods of liveness detection are explained. Pupil dilations are registered under various intensities of visible light and a feature vector is developed, measuring the distances between the movement's i.e. inner boundary and outer boundary of the image. Since the templates developed results in different values two groups of classifications are done, one is authentic and the other is fake. So, in order to achieve some values for fake classifications, some fake objects are also considered for results. Oscillations of pupil under different intensities of visible light results in this liveness detection

KEYWORDS: Spoofing, Impostor, Liveness Detection, Optical Characteristics, Purkinje Images, Intrinsic Properties, Involuntary Signals, Bodily Responses

Received: Mar 03, 2016; **Accepted:** Mar 14, 2016; **Published:** Mar 23, 2016; **Paper Id.:** IJCSEITRAPR20166

Original Article

INTRODUCTION

Automated Liveness Detection is a challenging research work going on nowadays. Liveness is a major attribute in individual's feature space but has very low specificity by itself, it is dichotomy of the feature space into live and non-living [4]. By presenting an artificial biometric attribute and scanning the fake, enhancing its quality using an enhancement algorithm, then that fake finger print is compared with a template and if it is matched, the impostor is accepted as a genuine [8]. Liveness detection reads claimant's physiological signs of life. Each trait like Face Recognition, thumb, Iris, lips, skin texture all have different methodologies to detect life in them which is being authenticated through Biometric device.

It is now widely acknowledged that biometric systems are vulnerable to manipulation. There are two forms of attacks which are referred to as direct and indirect. Direct attacks are also referred as spoofing or presentation attacks which are performed at the sensor level, outside the digital limits of a biometric system. Indirect attacks are

performed with in the digital limits by intruders such as cyber criminal hackers [6]. Biometric spoofing is a method of fooling a biometric system, where an artificial object (like a fingerprint mold) is presented to the biometric scanner that imitates the unique biological properties of a person which the system is designed to measure, so that the system will not be able to distinguish the artifact from the real biological target. Examples of Artificially created biometrics are image of a face or iris, lifted latent fingerprints, artificial fingers, high quality voice recordings etc [19].

LITERATURE SURVEY

In 2003 S. Schuckers et.al [1] proposed an algorithm quantifies the sweating pattern and makes a final decision about liveliness of the fingerprint by neural networks.

In 2004 John Daugman [2] proposed efficient algorithms for iris recognition and he proposed iris anti-spoofing counter measures.

Later in 2006, E. Lee, K. Park and J. kim [3] calculated the theoretical positions and distances between the Purkinje images based on the human eye model in their research.

S .Schuckers andB.tan in 2006 presented a new intensity based approach which quantifies the grey level differences using histograms and finds differences between live and fake fingerprint images [4].

Z. Wei, X. Qiu, Z. Sun in 2008 worked on Counterfeit Iris Detection based on texture analysis [24]. Textures printed on contact lens usually distribute over the outer half iris region, especially on the iris edge (transition from sclera to iris region). From the appearance of fake iris, it can be seen that its iris edge usually sharper than that of live iris. So they introduce Iris Edge Sharpness (IES) as the first measure to detect counterfeit iris

In 2009, the work of Kim et al. [5] is published as a paper in mask anti-spoofing. It aims to distinguish between the facial skins and mask materials by explaining the fact that their reflectance should be different. The distribution of albedo values for illumination at various wavelengths are analyzed to see how different facial skins and mask materials behave in reflectance.

X. He, Y. Lu, and P. Shi in 2009 [6] proposed a new fake iris detection method based on wavelet packet decomposition which is used to extract the features that provide unique information for discriminating fake iris from real ones and later Support vector machine(SVM) is used to characterize the distribution boundary.

In 2009, Z. He, Z. Sun, T. Tan, and Z. Wei worked on the properties that divide the iris into multiple regions. Each sub-region contains a particular texture pattern via such division, more specific representation of iris can be obtained, and hence makes it easier to discriminate live iris textures from counterfeit iris textures [22].

In August 2010 Gang Pan, Lin Sun, Zhaohui Wu and Yueming Wang [7] developed a non- intrusive face liveness detection system with the combination of eye blink and scene context. Anti spoofing clues i.e. both inside a face and outside a face are used in this system. Eye blinks are employed for anti-spoofing of photos and 3D models while the scene contexts are used for anti-spoofing of video replays.

In 2010, H. Zhang et al proposed a novel fake iris detection algorithm based on improved LBP and statistical features. Firstly, a simplified SIFT descriptor is extracted at each pixel of the image. Secondly, the SIFT descriptor is used to rank the LBP encoding sequence [25].

Younghwan Kim, Jang-Hee Yoo and Kyoungho Choi in May 2011 developed a Face Recognition system in which a motion and similarity-based fake detection algorithm is used for Liveness detection [8]. This approach is based on the idea that the amount of motion should be different obtained in a video sequence between fake and live situations.

In 2012, MaciejSmiatacz developed a new method to measure the liveness of face images using combination of optical flow estimation and SVM classifier [9]. It represents motion in a form of a vector field that allows transforming one image from the video sequence into the next one, by moving the blocks of the first image in the direction given by the vector field components. Even though this technique provides good results, motion field gets noisy when artificial objects are subjected to this technique.

Later Sebestian marcel in 2013 worked on Spoofing in 2D Face Recognition with 3D Masks and gave analysis on various Local Binary Patterns (LBP)-based anti-spoofing methods using color and depth images obtained from Kinect [10].

In 2014 Javier Globally, Sebastian Marcel added liveness assessment by using image quality assessment. They used extracted general image quality features to distinguish between genuine and constructed samples. It is a multitask and multi biometric protection method [11].

Adam Czajka, senior member of IEEE in April 2015 worked on pupil dynamics of eye [13]. He built his own database with a iris capture device and registered spontaneous pupil oscillations. He converts each observation by Kohn and clynes pupil dynamics model into feature space and later SVM is used for classification.

SPOOFING TARGETS

Every Biometric trait is considered as a target for spoofing. Creating different spoofing traits by using different materials are given below.

Fingers

By immersing subject's finger in impression material, create a mold. Molds can also be created from latent fingerprints by photographic etching techniques like those used in making of PCB (gummy fingers).Play-doh, gelatin, silicon or other suitable material are also used to cast a fake finger [1]. In worst case, a dead finger also helps in spoofing.

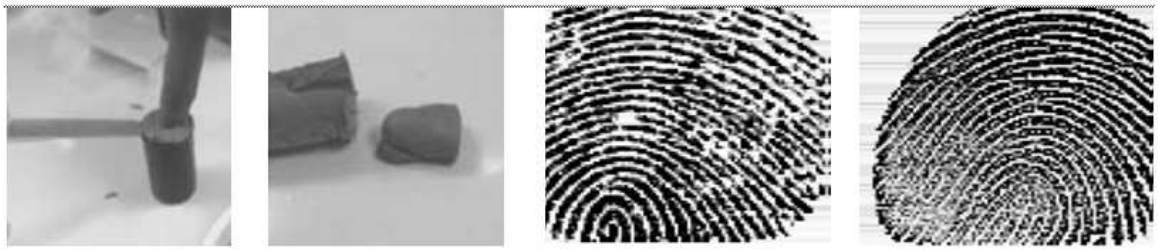

Figure 1: (a) Molds (b) Live Image (c) Dead Image

Face

A fraudster could fool or spoof a face recognition system using a photograph, video, dummy faces made of silica gel, rubber or a 3D mask bearing resemblance to a legitimate individual.

Figure 2: Examples of Fake Facial Specimens: From Left to Right Columns are Silica Gel, Rubber, Photos and Video Replay

Iris

Original images are captured for a better quality then they are printed on the paper using a commercial printer. The iris pattern may be printed on a plastic or rubber eye model which can be used at the iris sensor [15]. Next, the living eye may be the carrier for artificial contact lens with the iris pattern printed on it.

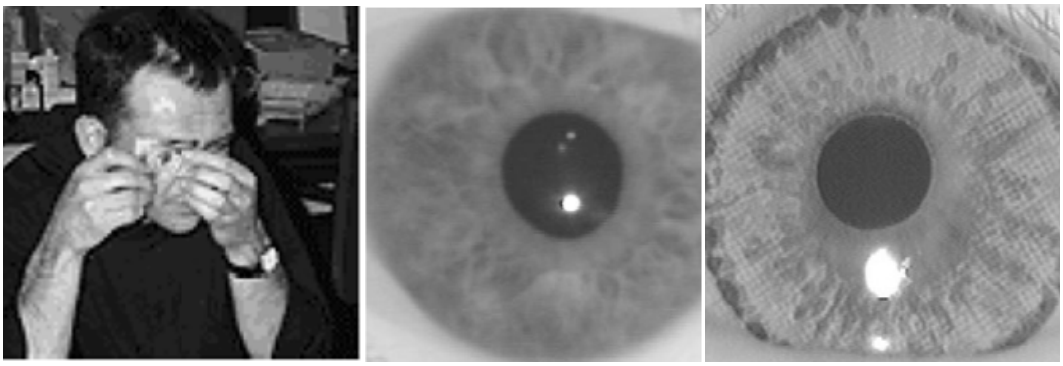

Figure 3: (a) Natural Iris (b) Fake Iris Printed on Contact Lens

Voice

The task of speaker verification system is to automatically verify a claimed identity based on a speech sample. Replay attack will be used to spoof a speaker verification system [12]. Replay attack is nothing but repeating a speech sample by using high quality voice recordings. Human voice mimicking can also be used, but it is not an efficient method.

Figure 4: Example of a Voice Recognition System

LIVENESS DETECTION

Liveness assessment methods represent a challenging problem as they have to satisfy certain demanding requirements [17].

- **Non-Invasive:** The technique should be beneficial for the individual or require an excessive contact with the user.
- **User Friendly:** People should be willing to use it.
- **Fast:** Results have to be produced in a very small time interval.
- **Performance**: It should have a good fake detection rate and should not degrade false rejection rate of a biometric system.

Liveness Detection for different Biometric traits is covered under three categories [15].

Intrinsic Properties of the Living Body

This includes the physical properties like density, elasticity, capacitance, resistance and analysis of body fluids; any biometric trait can be live detected by using these properties.

Involuntary Signals of Living Body

ECG for heart, hippus movements for iris, Blood pressure, pulse, brain, waves, blood flow are examples of involuntary signals. These properties are used for dynamic liveness detection.

Bodily Responses to External Stimuli

It is an effective liveness detection which requires user's involvement. The user is asked to shake the head, blink the eyes and pose various facial images, head movements and smile.

Its techniques can be divided into two groups.

In **Hardware based,** a specific device is added to the sensor to detect particular properties. In case of **Fingerprint**, temperature will be sensed, pulse detection on fingertip, pulse oximetry, Electrical conductivity etc will be considered [12].For **voice,** matching the lip movement (video) to the audio, specific reflection properties of eye will be considered for **iris** [14].

Figure 5: Pulse Oximeter

In **Software based**, a sample has been acquired with a standard sensor and features are used to distinguish between real and fake traits [15].

- **Fingerprint:** Perspiration pattern change between two or more fingerprints captured separated by some seconds.
- **Face:** Analyzing eyes blinking, studying head movements.
- **Iris:** Detection of hippus (pupil movement) and saccade (eye movement).

AUTOMATED PERSONAL IDENTIFICATION BASED ON IRIS LIVENESS DETECTION

Iris liveness detection can be done using physiological and optical characteristics of human iris [23]. In **physiological characteristics,** an eye itself has some Natural processes done by living things which can be used for liveness detection, Eye blink, pupillary light reflex, pupillary unrest (hippus), etc. Eye blink is a physiological activity of closing and opening eyelids which can be used for both face and iris liveness detection. Eye blink detection is useful to differentiate real iris from static fake iris patterns [5]. In the **optical characteristics** of human iris, real and fake irises exhibit different optical characteristics under visible, near-infrared (NIR), multispectral and structured lighting respectively. The main characteristics used for iris liveness detection under near infrared illumination include frequency distribution, Purkinje images, Image quality features, statistical texture features etc.

Pupil Dynamics

The Pupil is in the state of rhythmic contraction and dilation called hippus. Active illuminators are usually used in iris cameras to cause significant pupil dilation or constriction. Usually, Pupil size increases in a dark environment and decreases in a bright environment [12].

Adam Czajka in 2015 [13] built his own iris capture device to register pupil size changes under visible light stimuli, and registered 204 observations for 26 subjects (52 different irises), each containing 750 iris images taken every 40ms. Each measurement registers the spontaneous pupil oscillations and its reaction after a sudden increase of the intensity of visible light. Each observation is converted into a feature space defined by Kohn and Clynes pupil dynamics model [18] parameters and later Support vector machine (SVM) is used to classify natural reaction and spontaneous oscillations.

Red Eye Effect

Red eye effect is the common appearance of red pupils in color photographs of eyes [5]. It occurs when we use a photographic flash very close to the camera lens in ambient low light. This will be appeared in the eyes of humans and of animals as they contain tapetum lucidum [10].

In flash photography, the flash light that enters into the eye reflects back to the light source by retina. The camera records this reflected light. The main reason of the red color is the ample amount of blood in the choroid which nourishes the back of the eye and is located behind the retina [15].

Purkinje Image

Purkinje images are reflections of objects from the structure of the eye. They are also known as Purkinje reflexes. Conventional human eye has four optical surfaces; each of them reflects bright lights: the front and back surface of the cornea, and the front and back surface of the lens. In this case, the four reflected images of incident light on each optical

surface are called as Purkinje images [3]. The positions of these four Purkinje reactions depend on the geometry of the light sources. In his paper Lee et.al calculated the theoretical positions and distances between the Purkinje images based on the human eye model in their research [3]. The positions of these four Purkinje reactions depend on the geometry of the light sources. To overcome vulnerable issues of the Daugman method using Purkinje images, we consider the shaping model of the Purkinje image. As this model is designed with the Gullstrand eye model, the theoretical distances between the Purkinje images can be obtained. Because such distances are determined by human eye model the distances from genuine iris will vary from those of fake one. So, it's difficult to make fake iris that resembles the same distances of Purkinje images to those of live eye, as the material characteristics of fake iris is different to that of live iris. Since the first three Purkinje images (1st, 2nd and 3rd) are shaped by reflecting from a convex mirror, images are virtual and erect. But the last Purkinje image (fourth) is real and inverted as it is shaped by reflecting from a concave mirror [3]. Due to these facts, we know that the first two Purkinje images exist in symmetric position to 4th Purkinje image about the center of iris. Actually, the 3rd Purkinje image is made from anterior lens. But, the 3rd Purkinje image is not seen in image. Because the 3rd Purkinje image will happen on the behind position of an iris from the camera. Generally, a diameter of pupil is reported to be 2mm~8mm and its size is changed according to environmental light. When the light is stronger, the pupil size becomes smaller. In this case, since we use collimated IR-LED and its light is entered into the pupil area, the pupil size becomes the smallest (2mm). So, the iris area is enlarged consequently and the 3rd Purkinje image is concealed by an iris area in the image. Now, we introduce the method of calculating the distances between the first, second and fourth Purkinje images, theoretically. We can do the surfaces of posterior lens as concave mirror model. So, we can use the camera lens model. The sizes of Purkinje images are largest in each searching box. From that, the exact positions of Purkinje images can be detected excluding the noise by eyebrows, etc [3].

Iris Liveness Detection based on Quality Related Features

Considering the quality features, Galbally et al. proposed a liveness detection system based on a set of image quality related features[14].In the first step the iris is segmented from the background by using a circular Hough transform in order to detect the iris and pupil boundaries[20]. Iris printed images are a 2D surface in opposition to the 3D volume of a real eye for which acquisition devices are thought. The focus of a fake iris will vary from that of a genuine sample. The good focused image is a sharp image. Thus, defocus primarily attenuates high spatial frequencies, which means that almost all features estimating this property perform some measure of the high frequency content in the overall image or in the segmented iris region. It is expected that the degree of movement of an iris printed on a sheet of paper and held before a sensor will vary from that of a real eye where a more steady position can be maintained so that the small tremble observed in the first case should be almost imperceptible [14]. Motion-related features try to estimate the image blur of the iris or of the sensor (caused by motion). The effect of motion is generally reflected on the directionality, thus the estimators are usually depend on the computation of the preponderant directions within a given iris sample. A number of iris image quality features including focus features ,motion features, occlusion features, local and global contrast, pupil dilation are combined to construct a high dimensional feature vector for classification of fake and genuine iris images [14]. Pudil's Sequential Floating Feature Selection (SFFS) algorithm is used as feature selection method as it has a very good performance compared to other techniques [21]. For classification, a standard quadratic classifier fitting the training data with multivariate normal densities with diagonal covariance estimates stratified by group.

METHODOLOGY

Iris Recognition is considered as the most Authenticated and promising biometric trait when compared to other traits since it has specific features when compared to other organs of the human body. It has great mathematical advantage since iris patterns are unique from one person to another and also between left iris and right iris of the same person. In addition as an internal part of the eye, the iris is well protected and stays unchanged as long as one lives .Hence Iris recognition can be taken as a most promising biometric authentication. However Biometric recognition systems are vulnerable to be spoofed by fake objects. Potential threats for Iris based systems are

- **Eye Image:** Screen image, photograph, paper print, and video signal.
- **Artificial Eye:** Glass or plastic model.

Pupil is another promising authenticating part of the eye results in recognizing an impostor from a genuine. Iris liveness test can be done basing on the movements of the pupil. Basing on the fact that pupil size changes under visible light stimuli, values are registered basing on the spontaneous pupil oscillations and its reaction after a sudden increase of the intensity of the visible light [13]. Liveness detection test can be done externally by asking the subject to show eye movements and head movements. Different images were to be taken at different angles externally. Internally pupil dilations detect Iris liveness detection. Distance between each pupil movement is calculated and a feature vector is generated. Since each feature vector is identical to one another, the subject can be taken as a live subject. Since the live subject only has movements and different values.

CONCLUSIONS & FUTURE WORK

Nowadays, spoofing is a great threat to Biometrics. As a counterfeit, different anti-spoofing techniques came into existence. But the countermeasures affect user's convenience and hardware prices. In this paper, an overview of spoofing, anti-spoofing attacks and related techniques are presented. Some existing methods of Iris liveness detection are discussed. The present studies of anti-spoofing are very preliminary. With the advancement of technology, more research work has to be done in the area of liveness Detection.

REFERENCES

1. *R. Derakhshani et al. (2003).Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. Pattern Recognition, vol. 36, no. 2, pp. 383-396.*
2. *J. Daugman (2004).Iris recognition and anti-spoofing countermeasures. In Elsevier 7-th International Biometrics conference.*
3. *E. Lee et al. (2006). Fake iris detection by using Purkinje image. In Proc. ICB, Hong Kong, China, pp. 397–403.*
4. *B. Tan and S. Schuckers (2006).Comparison of ridge- and intensity-based perspiration liveness detection methods in fingerprint scanners. Proc. SPIE, 2006, pp. 62020A- 62020A. Biometric Technology for Human Identification III.*
5. *Y. Kim et al.(2009). Masked fake face detection using radiance measurements. Journal of the Optical Society of America A, 26(4):760–766.*
6. *X. He et al. (2009) .A new fake iris detection method. In Advances in Biometrics.ser. Lecture Notes in Computer Science, M. Tistarelli and M. Nixon, Eds. Springer Berlin Heidelberg, vol. 5558, pp. 1132–1139.*

7. *Gang Pan et al. (2010). Monocular camera-based face liveness detection by combining eye blink and scene context. TelecommunSyst.*
8. *Young wan Kim and Jang-HeeYoo (2011).A Motion and Similarity-Based Fake Detection Method for Biometric Face Recognition Systems. IEEE Transactions on Consumer Electronics, Vol. 57, No. 2.*
9. *Maciejsmiatacz (2012). Liveness measurement using optical flow for Biometric person Authentication. Metrology and Measurement systems, Vol. XIX (2012), No. 2, pp. 257- 268.*
10. *Sebastian Marcel and NesliErdogmus (2013). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. IEEE Sixth International Conference on Biometric Compendium.*
11. *Globally, Sebastian Marcel, Member and Julia Fierrez (2014).Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. IEEE Transactions On Image Processing, Vol. 23, No.2, February 2014.*
12. *Zhizheng Wu and HaizhouLi(2013).Voice conversion and spoofing attack on speaker verification systems. Signal and Information Processing Association Annual Summit and Conference (APSIPA), IEEE Asia-Pacific.*
13. *Adam Czajka, Senior Member, IEEE (2015). Pupil dynamics for iris liveness detection. IEEE Transactions on information forensics and security, Vol. 10, No. 4.*
14. *Javier Galballyet al (2012).Iris Liveness Detection based on Quality related features. Biometrics (ICB), 5th IAPR International Conference on Biometrics Compendium, IEEE.*
15. *Kezia R Badhiti and Prof. SudhaThatimakula. (2011).Spoofing- A threat to biometric systems. Journal of Computer Science and Engineering, Volume 7, issue 2.*
16. *Kezia R Badhiti and SudhaThatimakula (2013).Iris- An Emergent Biometric Technology for personal Authentication. International journal of Computer Science Engineering and Information Technology Research. Volume 3, issue 4.*
17. *RomyWadhwa (2014). Image Quality Assessment for fake biometric Detection. International journal for scientific Research & Development. Volume 2, Issue 3, ISSN: 2321-0613.*
18. *M. Kohn and M. Clynes (1969).Color dynamics of the pupil. Annals of New York Academy of Science, vol. 156, no. 2, pp. 931–950. Available online at Wiley Online Library.*
19. *Ma L et al. (2003).Personal identification based on iris texture analysis. IEEE Trans Pattern Anal Mach Intel 25(12):1519–1533.*
20. *R.T. Al-Zubi and D. I. Abu-Al-Nadi (2007).Automated personal identification system based on human iris analysis. Springer, Pattern Anal Applic 10:147-164.*
21. *P. Pudilet al. (1999).Adaptive floating search methods in feature selection. Elsevier Pattern Recognition letters,) 1157-1163.*
22. *Z. He et al. (2009).Efficient iris spoof detection via boosted local binary patterns. In Proc. ICB, Alghero, Italy, pp. 1080–1090.*
23. *Sebastien Marcel, Mark S. Nixon & Stan Z. Li (2014). Hand book of Biometric Anti-Spoofing. Advances in Computer Vision and Pattern Recognition: Springer London.*
24. *Z. Wei et al. (2008).Counterfeit iris detection based on texture analysis. In Proc. ICPR, Tampa, FL, USA, pp. 1–4.*
25. *H. Zhang et al. (2010).Contact lens detection based on weighted LBP. In Proc. ICPR, Istanbul, Turkey, pp. 4279–4282.*